BEFORE THE PUBLIC UTILITIES COMMISSION

OF THE STATE OF CALIFORNIA

FILED
03-09-10
04:59 PM

Order Instituting Rulemaking to Consider Smart Grid Technologies Pursuant to Federal Legislation and on the Commission's own Motion to Actively Guide Policy in California's Development of a Smart Grid System.	Rulemaking 08-12-009 (Filed December 18, 2008)

COMMENTS OF CISCO SYSTEMS, INC. TO ASSIGNED COMMISSIONER AND ADMINISTRATIVE LAW JUDGE'S JOINT RULING AMENDING SCOPING MEMO AND INVITING COMMENTS ON PROPOSED POLICIES AND FINDINGS PERTAINING TO THE SMART GRID

Jeffrey A. Campbell
Mary L. Brown
Cisco Systems, Inc.

1300 Pennsylvania Avenue, NW, Suite 250
Washington, DC 20004

Attorneys for Cisco Systems, Inc.

March 9, 2010

TABLE OF CONTENTS

I. INTRODUCTION..... 1

II. STANDARDS FOR REVIEW OF THE DEPLOYMENT PLANS SHOULD FOCUS ON POLICY OUTCOMES, ALLOWING UTILITIES TO ADDRESS THOSE OUTCOMES WITH DIVERGENT APPROACHES TO IMPLEMENTATION …….....5

III. THE COMMISSION SHOULD DEFER CONSIDERATION OF STANDARDS AND PROTOCOLS TO ANOTHER PROCEEDING, CONSISTENT WITH ITS OBLIGATIONS UNDER SECTION 8362(a)…….....9

IV. THE COMMISSION SHOULD WORK WITH INVESTOR-OWNED UTILITIES TO IDENTIFY INDUSTRY CYBER SECURITY BEST PRACTICES ANDENCOURAGE EVENT-RELATED INFORMATION SHARING…….13

V. CONCLUSION…….....19

I. INTRODUCTION

Pursuant to Rule 14.3 of the Commission's Rules of Practice and Procedure, Cisco Systems, Inc. ("Cisco") files these comments in response to Assigned Commissioner and Administrative Law Judge's Joint Ruling Amending Scoping Memo and Inviting Comments on Proposed Policies and Findings Pertaining to the Smart Grid (the "Ruling").

Cisco appreciates the opportunity to file comments in this proceeding. Cisco, headquartered in San Jose, California, is the worldwide market leader in Internet Protocol (IP)-based networking technologies. Cisco delivers an end-to-end, IP-based secure communications infrastructure for the smart grid from generation, transmission and distribution to businesses and homes. Cisco Smart Grid solutions help utilities:

- Optimize grid efficiency through better correlation of power supply and demand
- Reduce energy network outages and disruptions
- Increase the resiliency and security of the power system
- Increase environmental sustainability

Cisco believes that the CPUC, along with California utilities, technology companies, universities and others, is one of the states well-positioned to help the accelerate the nation's vision and implementation of Smart Grid. In particular, the CPUC's policies will be critical to ensuring utilities have the tools and the necessary regulatory environment to achieve the state's Smart Grid objectives. This proceeding, concerning Smart Grid deployment plans, provides an opportunity to grow that leadership.

The procedural requirements of SB17 require the California Public Utilities Commission (CPUC) to develop rules and requirements for the filing of Smart Grid deployment plans by

electric utilities, and calls upon the CPUC to evaluate deployment. Of course, even before this bill passed, the CPUC and the California electric utility industry were already implementing Smart Grid technologies and creating policies for the recovery of investment cost. SB17 can therefore be viewed as a legislative mandate to begin to consolidate, in a forward-looking plan form, information on investment already made and currently planned for the Smart Grid, along with the capabilities that the investment will enable. Putting this information in a forward-looking plan format should assist the CPUC to evaluate utilities' progress toward fulfillment of their plans, referencing the state's electric power policy articulated in Section 8360 of the law.[1]

The core questions raised in this proceeding revolve around how best the CPUC can make use of these deployment plans, and therefore asks questions about what the plans should contain and how they should be used in proceedings before the CPUC. In considering these questions, it is important to keep in mind that California utilities are implementing different Smart Grid technology platforms, in different domains, on different timelines, for different purposes, and potentially with different benefits. Cisco expects that, even when Smart Grid deployment is mature, the grid will be characterized by a variety of interoperable and scalable technologies. At this early stage, a deployment plan should be expected to capture the diversity of early Smart Grid deployments, and the CPUC should expect that the plans will evolve, in some cases in substantial ways, as the utility industry progresses in its efforts to implement the Smart Grid.

The Smart Grid, as described by the U.S. Department of Energy, is "[a]n automated, widely distributed energy delivery network, . . . characterized by a two-way flow of electricity and information and . . . capable of monitoring everything from power plants to customer preferences to individual appliances. It incorporates into the grid the benefits of distributed

[1] SB17, Chapter 327, Statutes of 2009.

computing and communications to deliver real-time information and enable the near-instantaneous balance of supply and demand at the device level."[2] This description begins to provide a sense of the multiple uses and purposes for a Smart Grid. Some of those uses will support regulatory mandates, such as the need to utilize renewable energy sources. Some of those uses will support improved management of the grid to support efficiency in power transmission and distribution, security, as well as new technology-enabled forms of conservation for consumers. The fulfillment of these diverse purposes, through network investment, will not happen simultaneously or instantaneously, but will be introduced over time.

When fully implemented, the Smart Grid will actually be a network of networks, much like the Internet in structure. For electric utilities, an architecture similar to the Internet, which is based on the Internet Protocol (IP) and is open and interoperable, is critical to achieving a Smart Grid. In Cisco's view, the Smart Grid, like the Internet, will require a control plane, which will be digitized using IP. In our view, such a control plane is best able to support wide scale interoperability, resiliency, and security issues that are critical to electric utilities.

Cisco supports an integration, and ultimately a migration, of existing technologies and solutions to an end-to-end, IP-based Smart Grid architecture.[3] IP-based architectures are scalable, extensible and reliable, and support both physical and cyber security solutions. They also enable backwards compatibility with legacy systems and networks, which is important for various reasons. First, it protects utilities' existing investments in information exchange technology, which both benefits ratepayers and avoids penalizing utilities for being Smart Grid

---

[2] "The Smart Grid: An Introduction," U.S. Department of Energy, at 17, *available at* http://www.oe.energy.gov/SmartGridIntroduction.htm.

[3] *See Internet Protocol Architecture for the Smart Grid*, Cisco Submission to the National Institute of Standards and Technology ("NIST"), (July 9, 2009), *available at* http://www.cisco.com/web/strategy/docs/energy/CISCO_IP_INTEROP_STDS_PPR_TO_NIST_WP.pdf (last visited March 5, 2010).

"early adopters." Second, backwards-compatibility allows Smart Grid product cycles to run their natural course, and prevents a potentially disastrous "hard stop" in equipment purchases that could result if utilities perceive an impending, specific technology mandate. Thus, while an IP-based system that leverages Internet architecture and new investment should be the ultimate goal, legacy systems must also be supported and migrated into an IP-based Smart Grid architecture over time. Perhaps the greatest benefit of an IP-based system is that an enormous and mature ecosystem exists, supporting advanced technologies that can accelerate the development of the Smart Grid.

Cisco's comments focus on three issues raised in the Ruling: (1) standards of review for the deployment plans (section 3.2), (2) standards and protocols that will support interoperability (section 3.5), and (3) cyber security (section 5.5). In the comments, below, Cisco demonstrates that:

- Deployment plans should be flexible to account for divergent approaches to implementing Smart Grid technologies;
- The CPUC should defer the immediate final adoption of standards and protocols and move to a separate proceeding that would further explore the most critical areas where standards are need and the status of standards work being developed by the organizations identified in SB17; and
- For cyber security, the CPUC should encourage best practices sharing with and among utilities, and explore public-private, security event-related information sharing.

II. STANDARDS FOR REVIEW OF THE DEPLOYMENT PLANS SHOULD FOCUS ON POLICY OUTCOMES, ALLOWING UTILITIES FLEXIBILITY TO ACHIEVE THOSE OUTCOMES WITH DIVERGENT APPROACHES TO IMPLEMENTATION

Section 3.2 of the Ruling poses questions about how the deployment plans should be reviewed by the CPUC. The Ruling states that SB17 requires the CPUC, in consultation with other stakeholders, to "determine the requirements" for utility deployment plans. The Ruling states that the law sets forth legislative policy for the grid,[4] and based on those policies, asks the CPUC and other relevant entities to "evaluate the impact of deployment on major initiatives and policies, and provides a list of those initiatives such as meeting California's needs for renewable sources of energy, energy efficiency, and demand response goals.[5] Drawing from those two

[4] Section 8360 of SB17 declares state policy is to modernize the grid to maintain safe, reliable, efficient, and secure electrical service, while meeting future growth needs of the state, through (a) Increased use of cost-effective digital information and control technology to improve reliability, security, and efficiency of the electric grid; (b) Dynamic optimization of grid operations and resources, including appropriate consideration for asset management and utilization of related grid operations and resources, with cost-effective full cyber security; (c) Deployment and integration of cost-effective distributed resources and generation, including renewable resources; (d) Development and incorporation of cost-effective demand response, demand-side resources, and energy-efficient resources; (e) Deployment of cost-effective smart technologies, including real time, automated, interactive technologies that optimize the physical operation of appliances and consumer devices for metering, communications concerning grid operations and status, and distribution automation; (f) Integration of cost-effective smart appliances and consumer devices; (g) Deployment and integration of cost-effective advanced electricity storage and peak-shaving technologies, including plug-in electric and hybrid electric vehicles, and thermal-storage air-conditioning. (h) Provide consumers with timely information and control options; (i) Develop standards for communication and interoperability of appliances and equipment connected to the electric grid, including the infrastructure serving the grid; (j) Identification and lowering of unreasonable or unnecessary barriers to adoption of smart grid technologies, practices, and services.

[5] Section 8366 of SB 17 contains the statutory criteria the CPUC should use to evaluate deployment by utilities of the smart grid: (a) Implementation of new advanced metering initiatives; (b) Achievement of the renewables portfolio standard program requirements and the need to operate the smart grid of the future with a substantial increased percentage of electricity generated by eligible renewable energy resources; (c) Achievement of state goals for reducing emissions of greenhouse gases as set forth in the California Global Warming Solutions Act of

sections of the law, the Ruling proposes a list of eight requirements for a Smart Grid, and asks whether the deployment plans should explain how the utilities' deployments will advance those eight requirements: (1) grid that is self-healing and resilient; (2) motivate consumers to change behavior, including allowing pricing to increase in peak periods; (3) grid must resist attack; (4) provide more stable and reliable power, including reduction of downtime; (5) accommodate all generation and storage options; (6) enable electricity markets to flourish; (7) run more efficiently by minimizing operational and maintenance cost; and (8) enable penetration of intermittent power generation sources. The Ruling proposes that each plan should include (1) a "demonstrable vision" of the Smart Grid, which would include how a utility's vision for the Smart Grid would perform in each of the eight enumerated areas; (2) a timeline; and (3) projected cost, to the extent possible at this time.

In Cisco's view, requirements for deployment plans should be sufficiently flexible to allow for differences in breadth and specificity, and the CPUC's expectation should be that deployment plans will be modified over time as new solutions become available to utilities. CPUC acceptance of a deployment plan should not be elevated to the equivalent of a decision in rate cases about whether actual investment furthers the legislative principles listed in SB17. While the CPUC's execution of Section 8366 ultimately must occur in the context of rate cases in which actual deployments are reflected in the proposals made by the utility for the recovery of costs, the law does not mandate the fulfillment of Section 8366 in deployment plans.

2006 and other state directives; (d) Achievement of the energy efficiency and demand response goals as required by Sections 454.5 and 454.55 and other state directives; (e) Modernizing the aging utility grid infrastructure; (f) Meeting the future energy growth needs of the state with new and innovative technologies and methods that utilize the existing assets more efficiently, result in a less environmentally adverse net impact on the state, meet stringent costs versus benefit assessments, and provide the ratepayers with new options in meeting their individual energy needs; (g) Implementation of technology to improve worker safety, protection, and productivity.

That said, as a vision statement and a planning tool, deployment plans containing information about how a utility will address these topics is a useful means to ensure that there is policy agreement between a regulated utility and the CPUC on what is important in the deployment of the Smart Grid. The regulator needs to specify what is important to it in the deployment of the Smart Grid by stating broad policy outcomes the state wants to achieve, and the utility needs the flexibility to produce those outcomes in a way that makes sense for its operations and customers. Discussing those plans in a written document can assist the CPUC in preparing for future rate cases, or in identifying other policy issues that the CPUC may need to address as deployment advances. As the CPUC noted, the level of specificity of these plans should be at a high level, and not be of the level or type of information that one might expect in a General Rate Case.[6] The plan should be informative of the future direction that the utility expects to take, without locking the utility in to the execution of its vision document. Technology and innovation are moving too fast in this area to permit a utility to determine its ultimate deployments as of 2010. Cisco also agrees that annual updates of the plan would be helpful, since it is likely that plans will be modified over time.

Cisco is concerned that the language in the Ruling suggests that utility must achieve *all* of the objectives outlined by the legislature for its Smart Grid deployment. For example, the CPUC tentatively proposes that, "We propose that in filing their deployment plan, IOUs should discuss in detail how their vision of Smart Grid will perform in *each* of the areas stated above, particularly with reference to the relevant sections of § 8360 and § 8366."[7] In Cisco's view, the statute does not require that each utility address every legislative objective in SB17 as part of its deployment plan. Section 8360 states California legislative policy, and at Section 8366, SB 17

[6] *See* Ruling at 6, 7.
[7] *See* Section 3.2 of the Ruling, at 13 (emphasis added).

requires that actual deployments be evaluated for consistency with state initiatives listed in that section.[8] A utility should be given flexibility in crafting its deployment plan to take into account the legacy assets in each utility system, as well as specific attributes of its operations and its service territory, including its consumer base, the current state of its network, its overarching business objectives and the state of the technology. Utilities should have flexibility in timing and staging proposed deployments of Smart Grid technologies in a manner that makes the most business sense.

Cisco's expectation is that over time, utilities will continue to migrate Smart Grid capabilities toward an IP control plane, and that devices, solutions, and technologies enabling the grid to be smart, will eventually be IP-based. But there is too much legacy technology to simply flash-cut to that IP future. For the near-term, Cisco expects that utilities will increasingly use IP networks to link legacy systems together, which will improve the functionality of legacy systems themselves by improving observability of data in the grid, and to begin to introduce IP-based technologies into different domains of the grid over time, such as IP-based technologies that can be deployed in the home for demand response purposes.

In sum, CPUC compliance with Section 8366 ultimately must occur in the context of rate cases in which actual deployments are reflected in the proposals made by the utility for the recovery of costs. Deployment plans, in contrast, should allow for differences in breadth and specificity, and the CPUC's expectation should be that deployment plans will be modified over time as new solutions become available to utilities.

[8] Section 8366: "The commission…shall evaluate the impact of *deployment* on major initiatives and policies, including…." (emphasis supplied). The introduction used the term "deployment" and not "deployment plans."

III. THE COMMISSION SHOULD DEFER CONSIDERATION OF STANDARDS AND PROTOCOLS TO ANOTHER PROCEEDING, CONSISTENT WITH ITS OBLIGATIONS UNDER SECTION 8362(a)

In Section 3.5, the Ruling notes that the groups identified in Section 8362 of SB 17 have not yet adopted protocols and rules to ensure functionality and interoperability of the Smart Grid. The Ruling considers several approaches to meeting its statutory obligations, and invites public comment on them, including (1) deferring CPUC consideration in this proceeding until a number of the listed groups have adopted standards or protocols; (2) deferring CPUC consideration of such matters to another proceeding that would begin after a number of the listed groups have adopted standards; or (3) adopting a "performance standard" in this proceeding requiring that those implementing Smart Grid technology take steps to ensure that the technology has the capability to function and operate with devices developed pursuant to standards adopted by the listed groups.[9]

Cisco provides standards-based technology and solutions, and appreciates the Ruling's consideration of various approaches to ensure that a common set of standards and protocols are adopted and utilized in building-out California's Smart Grid. In doing so, the Ruling is promoting the public interest by ensuring that the new interoperable technologies deployed in the Smart Grid are "future-proof" and innovative, because interoperability facilitates the introduction of new technologies and solutions as the needs and functions of Smart Grid evolve over time.

Cisco believes that the CPUC should defer its consideration of standards and protocols to another proceeding that will commence after a number of the listed agencies have adopted standards or protocols. Cisco recommends that the CPUC should (a) consider the standards identified the final National Institute of Standards and Technology (NIST) Framework and

[9] *See* Ruling, Section 3.5, at 18-19.

Roadmap for Smart Grid Interoperability Standards, Release 1.0" ("NIST Interoperability Framework"), which was published on January 20, 2010,[10] and; (b) identify those areas where the CPUC determines, based on stakeholder input, that the CPUC's adoption of standards and protocols is warranted in order to ensure common functionality and interoperability, and to promote the public interest. For example, while the final NIST Interoperability Framework includes IP and other interoperable standards and protocols that we believe will serve as the platform to enable Smart Grid functionality, NIST explained in its press release announcing final publication, "…some of the standards listed in the NIST report are still under development and some others, such as those already used voluntarily by industry, *may not warrant adoption* by FERC or other regulators."[11]

Consistent with our belief that progress towards shared goals can be accelerated through collaboration, Cisco is an active participant and leader in many national and international standards-development organizations (SDOs), as well as in the NIST Smart Grid interoperability standards process. Through our participation in the GridWise Alliance, Cisco supported provisions in the Energy Independence and Security Act of 2007 which state, "The Director of the National Institute of Standards and Technology shall have primary responsibility to coordinate the development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems."[12] Cisco has provided specific technical input to NIST throughout the first and second phases of NIST's Smart Grid activities.

---

[10] NIST Framework and Roadmap for Smart Grid Standards, Release 1.0, NIST Special Publication 1108 (Jan. 20, 2010), (emphasis added), *available* at http://www.nist.gov/public_affairs/releases/smartgrid_interoperability_final.pdf.

[11] "NIST Issues First Release of Framework for Smart Grid Interoperability," Jan. 19, 2010, *last accessed on Mar. 5, 2010 at* http://www.nist.gov/public_affairs/releases/smartgrid_011910.html

[12] Energy Independence and Security Act of 2007, § 1305, 15 USC § 17385(a) (Supp. 2009)

During Phase 1, Cisco participated in a number of stakeholder workshops to help NIST identify existing standards used in the current electrical grid, determine the main use cases for Smart Grid and proposed that NIST consider using an Internet architecture, which uses the Internet Protocol (IP) suite of standards, as the framework for the new Smart Grid architecture. Cisco also provided comprehensive input to NIST in response to a *Federal Register* notice requesting public comment on the initial list of interoperability standards.[13]

Cisco further noted that when the new IP-based architecture is initially deployed, the total build-out may in fact be smaller than the existing proprietary networks and do nothing but interconnect them. The legacy proprietary networks will continue to operate as long as the utility considers them useful. However, new IP-based build-outs would use the interoperable architecture, and with an ecosystem of vendors competing to sell their offerings, utilities will benefit from competitive pricing, even as vendors compete based on functional differentiation. In time, the IP-based interoperable architecture therefore dwarfs the legacy proprietary networks. Cisco suggested to NIST that the use of IPv6 would minimize the possibility of utilities deploying technologies that are obsolete upon installation, which we also urge the CPUC to take into account.

Cisco summarized for NIST the many benefits that using the Internet Architecture as a basis for Smart Grid interoperability would bring, such as:

- Increased competition among Smart Grid vendors and service providers, which will help accelerate innovation and result in competitive prices;
- Enhanced logical and physical security, which will help secure our nation's critical infrastructure;

[13] *NIST Initial List of Smart Grid Interoperability Standards; Request for Comments*, Federal Register: June 9, 2009 (Volume 74, Number 25).

- High reliability and resiliency, which will aid utilities in managing, maintaining and upgrading their Smart Grid system; and
- Increased flexibility, scalability and manageability, which will drive to new business models and customer empowerment.

During Phase 2, Cisco again provided detailed input to NIST in response to another *Federal Register* notice[14] requesting public comment on the draft NIST Smart Grid Interoperability Standards Framework and Roadmap. In the draft, NIST had not yet identified the suite of IP-based standards and protocols in its list of Smart Grid interoperability standards. Cisco again made the case for IP and also commented on a number of standards and protocols that we believed did not provide the interoperability necessary to meet the needs of a dynamic Smart Grid with millions of addressable end-points to be managed and secured. Cisco is pleased to report that NIST identified IPv4, IPv6 and the core suite of IP standards and protocols in its final NIST Interoperability Framework. At the same time, NIST listed 50 "Additional Standards, Specifications, Profiles, Requirements, Guidelines, and Reports for Further Review,"[15] some of which Cisco believes warrant inclusion among the 25 "Standards Identified by NIST."[16] For example, IEEE 802.11 Wireless LAN Medium Access Control and PHY layer is a standard – commonly referred to as "WiFi" – that provides secure, managed, radio-based data communications supporting a variety of data rates, ranges, and power consumption profiles. The 802.11 standard is listed in the NIST Interoperability Framework "for further review."[17] 802.11 is directly relevant to the use cases analyzed for the Smart Grid, especially the Home Area

---

[14] *Draft NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0; Request for Comments*, Federal Register: October 9, 2009 (Volume 74, Number 195).
[15] Id, Table 4-2 at pp. 62-73.
[16] Id, Table 4-1 at pp. 50-60.
[17] Id, Table 4.2, #11 at p. 64.

Network and the Neighborhood Area Network. Wi-Fi has become a ubiquitous technology, used today by an estimated 1 in every 10 people worldwide and having shipped approximately 2 billion units in the ten years since its initial commercialization. It is estimated that the 2 billionth chipset shipped in 2009 and that about 1.6 million Wi-Fi chips ship each day. Moreover, the stability of the Wi-Fi standards is evidenced by the fact that there are over 6,000 product certifications, and demonstrating one of the most successful multivendor interoperability programs ever established.

Although IEEE 802.11 was not listed among the "Standards Identified by NIST," SB17 specifically references the IEEE, which we believe would include IEEE 802.11, thereby giving the CPUC and California utilities a broader set of technology choices than the current list from the NIST provides. Cisco is working within the NIST process to improve its list over time.

Interoperability increases utility and consumer choice in what technologies to invest in and helps ensure that future investments are deployable. Cisco believes that the CPUC should delay its adoption of standards and initiate a separate proceeding to determine in which functional areas and for what purposes CPUC standards adoption is warranted, and to evaluate the status of standards under development by the listed entities.

IV. THE COMMISSION SHOULD WORK WITH INVESTOR-OWNED UTILITIES TO IDENTIFY INDUSTRY CYBER SECURITY BEST PRACTICES AND ENCOURAGE EVENT-RELATED INFORMATION SHARING

In Section 5.5, the Ruling asks what cyber security principles Smart Grid proposals should meet. The Ruling describes public concern about the security and privacy of the Smart Grid system data and individual consumer data. The Ruling also notes that the CPUC has received information about how smart meters will generate thousands of data points from each

home and how such data could be used to develop profiles of house occupancy and could leave homeowners vulnerable to theft. The Ruling asserts that cyber security is an issue with many dimensions, referring to recent media articles about how common cyber attacks have become on our nation's infrastructure, and noting that the CPUC's policy to allow authorized third-parties to access customer data could also open the possibility that customer information could be accessed by third-parties without that customer's consent. The Ruling summarizes the positions of various parties in this proceeding.

In discussing security, the Ruling indicates that it's unclear whether current efforts to protect information and utility infrastructure are adequate, as well as the extent to which federal security standards would sufficiently protect California's grid. The Ruling supports a clear, flexible approach to security and privacy standards adopted in California, and observes that implementing state or federal standards is complicated with multiple Smart Grid market participants which have different security capabilities, limitations and proprietary tools. Finally, the Ruling asks a series of questions about (a) whether the CPUC, as part of its funding criterion, should require Smart Grid project proponents to verify that the project conforms with state or federal security and privacy standards, and (b) whether the CPUC should undertake special reviews of Smart Grid privacy and security. As stated in the Ruling, "…any standards eventually adopted in California must be both comprehensible and flexible enough to encompass emerging security threats and risks, as well as protecting privacy. This is especially important as new technologies and information systems are deployed."[18]

As an initial matter, while security and privacy are often discussed together – particularly with respect to ensuring that individual or household data is transmitted and stored securely – they are distinct. The former relates to the people, processes and technologies used to mitigate

[18] *See* Ruling, Section 5.5.2 at p. 38.

the threats against physical, cyber, or information assets, while the latter relates to rules relating to the collection, transfer, or management of personal or sensitive information. From a policy perspective, it's important not to conflate the two, as the challenges and solutions are unique to each area.

Innovation in both cyber and physical security technology, best practices sharing and event-related information sharing among public and private entities are critical elements to a comprehensive strategy that the state and California IOUs may want to keep in mind as they work together to mitigate security threats and protect consumer privacy. There is not one technology or approach that will secure the Smart Grid completely; however, there are industry best practices and approaches to public-private partnership that have proved effective and valuable in addressing security threats to other communications systems. Perhaps the best example of a successful public-private partnership focused on best practices and information sharing to protect critical communications infrastructure is the National Coordinating Center for Communications (NCC). In 1982, telecommunications industry and Federal government officials identified the need for a joint mechanism to coordinate initiation and restoration of national security and emergency preparedness (NS/EP) telecommunication services. In 1983, the group recommended to the National Security Telecommunications Advisory Committee (NSTAC) and to the President that a joint industry and government-staffed NCC be created as a central organization to handle emergency telecommunication requests. On January 3, 1984, the NCC opened for business. Today, the NCC is home to representatives from 24 Federal departments and agencies and 40 telecommunications companies and associations.[19] The NCC's industry and government representatives use the NCC's unique organization to work together

[19] *See* http://ncs.gov/ncc/gov_ind.html

during day-to-day operations, coordinate NS/EP responses during crises, and produce emergency response plans and procedures as a result of lessons learned during actual events.

In January 2000, the NCC was designated an Information Security Advisory Committee (ISAC) for Telecommunications in accordance with Presidential Decision Directive (PDD)-63.[20] The NCC-ISAC facilitates the exchange among government and industry participants regarding vulnerability, threat, intrusion, and anomaly information affecting the telecommunications infrastructure.

With the advent of Smart Grid, the CPUC and IUOs have an opportunity to work together to "bake-in" security from the outset, as new technologies are brought online. Cisco strongly believes that the integration of IP-based Smart Grid technologies will help make the grid more secure if properly implemented and managed. Cisco has demonstrated experience and success with this model. Consider the public switched telephone networks (PSTNs) that support the traditional telephone services which most homes and businesses use. As communications networks migrate to IP technology, network operators are using network segmentation and design controls to ensure that critical elements of this infrastructure (call managers, voicemail servers, and so on) are not openly exposed and vulnerable to the open Internet. As further validation, we continue to see increasing adoption rates for IP-based telephony deployments. With respect to the grid, we understand that one area of concern with IP migration is simply that because IP is standards-based, there is a larger community that potentially understands how to exploit vulnerabilities in the protocol. However, by adopting the principles of network security, this risk can be mitigated with a strategy that involves a combination of people, process, and technology. Moreover, substantial peer-review and significant investment by security experts and organizations provide a firm foundation for standards-based security technology.

---

[20] *See* http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

It's also worth noting IP made the Internet possible, but IP is not the Internet. The Internet is a "network of networks" that uses IP and the Internet architecture. It is not the only network that does so: Corporate networks are typically private networks that also use IP, but physically connect to the Internet only at certain well-secured points. Various militaries also run IP networks that do not connect to the Internet at all. The Internet will likely be used in the Smart Grid to provide customers with energy information on home, business, and portable devices and allow them to set configurable energy parameters, but Internet interconnectivity to the Smart Grid will be limited to specific energy functions.

Cisco's vision for Smart Grid security is based on principles learned from years as the world leader in building secure data networks:

- Maximize utility visibility into the network environment, devices and events.
- Control network users, devices, and traffic.

The Cisco Smart Grid security vision takes a zone-based approach in which each security zone encompasses a discrete Smart Grid business function or operation. Cisco has identified four security zones to protect the major functions of the Smart Grid: customer operations; corporate; home/business area network; and telemetry and control systems.[21] These security zones follow established industry practices for delivering energy to customers, and protect assets for power generation, transmission, and distribution, as well as the "last mile" to energy consumers' premises. This zone-based model supports multiple utilities managing different parts of the grid, and provides a grid protection scheme that is independent of topology or network transport.

[21] These principles are detailed in Cisco's Secure Architecture for Enterprise (SAFE). Cisco applies these principles to the unique environment and demands of the smart grid to create a converged, modular security platform that provides fast response to threats and helps ensure regulatory security policy compliance while reducing operating and management expenses.

Explained in greater depth in a Cisco-authored White Paper on Securing the Smart Grid,[22] the above vision provides the foundation for Cisco's approach to Smart Grid security, and illustrates the type of information and best practices sharing that could be exchanged with and among utilities. Moreover, we believe that the CPUC may want to confer with the North American Electric Reliability Corporation (NERC) to explore ways to create a state-level public-private mechanism to share security event-related information, based on the NERC model of the national-level Electricity Sector Information Sharing and Analysis Center (ES-ISAC)[23], which could help not only mitigate against current attacks, but could also serve as a venue to discuss ways to mitigate against the threat of future attacks.

Cisco would encourage the CPUC to consider the role of innovation when developing any standards or policies related to addressing security threats to the Smart Grid. In the majority of cases, specific standards and policies that lock-in technologies or security approaches can have negative, unintended consequences. We urge the CPUC to find a non-invasive and least-prescriptive means to work with industry to ensure that the threats to Smart Grid security are mitigated.

Cisco welcomes and echoes the Ruling's observation that any potential or eventual standards must be easy to implement and flexible, and we would be pleased to provide the CPUC further information about Cisco's vision and strategies to enable Smart Grid security. We believe that best practices sharing and information exchange are important tools in building a robust, secure Smart Grid in California.

---

[22] "Securing the Smart Grid," White Paper, Cisco Systems, Inc., (2009), *available at* http://www.cisco.com/web/strategy/docs/energy/SmartGridSecurity_wp.pdf .
[23] http://www.esisac.com/

V. CONCLUSION

Cisco appreciates the opportunity to comment on this proceeding and looks forward to working with the CPUC and other stakeholders on these important issues.

Respectfully submitted,

Cisco Systems, Inc.

By: */s/* Jeffrey A. Campbell

Jeffrey A. Campbell
Mary L. Brown
Cisco Systems, Inc.
Government Affairs
1300 Pennsylvania Avenue, NW, Suite 250
Washington, DC 20004

March 9, 2010

CERTIFICATE OF SERVICE

I, Eric Gunning, hereby certify that, pursuant to the Commission's Rules of Practice and Procedure, I have this day served a true copy of **COMMENTS OF CISCO SYSTEMS, INC. TO ASSIGNED COMMISSIONER AND ADMINISTRATIVE LAW JUDGE'S JOINT RULING AMENDING SCOPING MEMO AND INVITING COMMENTS ON PROPOSED POLICIES AND FINDINGS PERTAINING TO THE SMART GRID** to each party named in the official service list for Proceeding R. 08-12-009 by delivering a copy via electronic mail to each party named in the official service list and mailing a properly addressed copy by first-class mail with postage prepaid to each party in the official service list without an electronic mail address.

Executed on March 10, 2010 at Denver, Colorado.

/s/ Eric Gunning
Eric Gunning
Wilkinson, Barker, Knauer, LLP
1515 Arapahoe Street
Tower 1, Suite 1600
Denver, CO 80202
egunning@wbklaw.com